APPLICATION UNDER UNITED STATES PATENT LAWS

Atty. Dkt. No. PW 0275038
(M#)

Invention: DYNAMIC CONFIGURATION OF OF IPSEC TUNNELS

Inventor (s): GREWAL, Karanvir
GEORGESCU, Cristina

Pillsbury Winthrop LLP
Intellectual Property Group
1600 Tysons Boulevard

McLean, VA 22102
Attorneys
Telephone: (703) 905-2000

This is a:

- ☐ Provisional Application
- ☒ Regular Utility Application
- ☐ Continuing Application
  - ☐ The contents of the parent are incorporated by reference
- ☐ PCT National Phase Application
- ☐ Design Application
- ☐ Reissue Application
- ☐ Plant Application
- ☐ Substitute Specification
  Sub. Spec Filed _____
  in App. No. ____/_____
- ☐ Marked up Specification re
  Sub. Spec. filed _____
  In App No ____/_____

SPECIFICATION

DYNAMIC CONFIGURATION OF IPSEC TUNNELS

BACKGROUND

1. Field

[0001] The present invention relates generally to virtual private networks (VPNs). Specifically, the present invention relates to methods and systems for configuring VPN tunnels.

2. General Background and Related Art

[0002] In the age of electronic communications, it is essential that parties communicate with each other in a secure, protected manner. Absent appropriate security measures, external parties may gain access to information exchanged between communicating parties. Such access may compromise both public and private interests.

[0003] Security technologies have emerged to address problems inherent in electronic exchanges of information. For example, a virtual private network (VPN) is a secure network connection within a network. Specifically, a VPN "tunnel" is a secure connection established between endpoints in a network. All data exchanged between a node at a first endpoint and a node at a second endpoint is subject to some kind of security manipulation, such as encryption. As such, an external party may not gain access to the data exchanged. Nodes may be geographically remote, separated by many intervening switches and routers.

[0004] To establish a VPN tunnel, an initiator and a responder may participate in a series of negotiations. The initiator may initiate a negotiation with the responder. During the negotiation, information may be exchanged between the nodes that sets forth security policies

applicable to future exchanges of information. Where several phases of negotiation occur, a secure set of defining parameters may be generated. Thus, a tunnel may be established, and the initiator and the responder may communicate in a secure manner.

[0005] Protocols govern the process of establishing tunnels between nodes. Specifically, IPSec, RFC 2401, 2411, is a set of extensions to the IP protocol family that enables the creation of encrypted tunnels. IPSec provides cryptographic security services, including authentication, integrity, access control, and confidentiality support. IPSec is transparent to network applications. The protocols and rules governing IPSec transmissions must conform to documents promulgated by Internet working groups.

[0006] IPSec includes a number of protocols, including Authentication Header (AH), RFC 2402, and ESP (Encapsulated Security Payload), RFC 2406. IPSec-secured links are defined in terms of security associations (SAs), RFC 2408. An SA is a security configuration that includes information required for execution of various network security services. In particular, an SA may include security attributes, such as network parameters and network addresses. Each SA is defined for a single unidirectional flow of data, usually from a single node to another node, and covers traffic distinguishable by some unique selector. The applicable security protocol for SAs may be AH or ESP. The AH follows a basic IP header and contains cryptographic hashes of the data as well as identification information. The ESP header allows for rewriting of the payload in encrypted form.

[0007] FIG. 1 (Prior Art) depicts a system in which a tunnel may be established. System 100 includes a client 120 and a gateway 180 which communicate with each other over the Internet 160. Client 120 stores the IP address 130 of gateway 180. Client 120 also stores a security configuration 140. Similarly, gateway 180 stores a security configuration 170.

[0008] In order to establish a tunnel 150 between client 120 and gateway 180, client 120 may initiate a preliminary negotiation with gateway 180. In this preliminary negotiation, client 120 and gateway 180 may agree upon a security algorithm to use in subsequent negotiations. In the IPSec protocol, this preliminary negotiation is termed phase1 negotiation. After phase1 negotiation, client 120 may initiate another negotiation with gateway 180. In what is termed phase2, client 120 and gateway 180 generate secure keys to define subsequent secure transmissions between client 120 and gateway 180 over tunnel 150.

[0009] Phase2 negotiation only succeeds if gateway 180 and client 120 are identically configured. That is, to establish tunnel 150, security configuration 170 in gateway 180 must be identical to security configuration 140 in client 120. If even a slight difference exists between the respective security configurations, phase2 negotiation fails.

[0010] Accordingly, a client administrator 101 must configure parameters within security configuration 140. Similarly, a gateway administrator 110 must configure security parameters within security configuration 170. This configuration process is complex, and client administrator 101 must know the respective security configuration of every endpoint with which client 120 seeks to establish a tunnel. Moreover, when gateway administrator 110 alters even one parameter within security configuration 170 of gateway 180, client administrator 101 must modify the counterpart parameter within security configuration 140 of client 120. FIG. 2 (Prior Art) depicts exemplary security configurations that may be associated with client 120 and gateway 180 in FIG. 1.

[0011] Therefore, what is needed is a method and system for dynamically configuring tunnels in a network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 (Prior Art) illustrates a system in which a tunnel may be established.

[0013] FIG. 2 (Prior Art) depicts security configurations that may be associated with a client and a gateway in the system of FIG. 1.

[0014] FIG. 3 illustrates a system according to an embodiment of the present invention.

[0015] FIG. 4 is a high-level flow diagram of a method according to an embodiment of the present invention.

[0016] FIG. 5 is a high-level flow diagram of a method according to an embodiment of the present invention.

[0017] FIG. 6 is a high-level flow diagram of a method according to an embodiment of the present invention.

[0018] FIG. 7 illustrates an exemplary Configuration Mode Exchange transaction.

DETAILED DESCRIPTION

[0019] The following detailed description refers to the accompanying drawings that illustrate exemplary embodiments of the present inventions. Other embodiments are possible and modifications may be made to the embodiments without departing from the spirit and scope of the invention. Therefore, the following detailed description is not meant to limit the invention. Rather, the scope of the invention is defined by the appended claims.

[0020] It will be apparent to one of ordinary skill in the art that the embodiments as described below may be implemented in many different embodiments of software, firmware, and hardware in the entities illustrated in the figures. The actual software code or specialized control hardware used to implement the present invention is not limiting of the present invention. Thus, the operation and behavior of the embodiments will be described without specific reference to the actual software code or specialized hardware components. The absence of such specific references is feasible because it is clearly understood that artisans of ordinary skill would be able to design software and control hardware to implement the embodiments of the present invention based on the description herein with only a reasonable effort and without undue experimentation.

[0021] Moreover, the processes associated with the presented embodiments may be stored in any storage device, such as, for example, a computer system (non-volatile) memory, an optical disk, magnetic tape, or magnetic disk. Furthermore, the processes may be programmed when the computer system is manufactured or via a computer-readable medium at a later date. Such a medium may include any of the forms listed above with respect to storage devices and may further include, for example, a carrier wave modulated, or otherwise manipulated, to convey instructions that can be read, demodulated/decoded and executed by a computer.

[0022] A method and system for dynamically configuring a tunnel, as presented herein, involves a client and a gateway. The client initiates a negotiation with the gateway. The gateway sends information to the client. The client extracts a security configuration from the information sent by the gateway. Using the security configuration, a tunnel between the client and the gateway is established.

[0023] Accordingly, a minimal configuration may be defined on a client. A gateway administrator may modify network attributes on the gateway, as well as security policies with respect to peers, users, and groups, without manually conveying the modifications to a client.

[0024] FIG. 3 illustrates system 300 according to an embodiment of the present invention. As shown, system 300 comprises a client 320 and a gateway 380 communicating over the Internet 360. For illustrative purposes, tunnels are shown herein as being formed between clients and gateways. The term "client" corresponds to a first endpoint of a tunnel, and "gateway" corresponds to a second endpoint. These terms may encompass any of a number of devices, such as personal computers, client computers, servers, mainframes, gateways, personal digital assistants (PDAs), other handheld devices, and other computing devices. The terms "first peer" and "second peer" may be substituted for "client" and "gateway." Additionally, the Internet 360 may be replaced by another network, such as an intranet.

[0025] Gateway 380 stores or has access to a security configuration 370, which may comprise security and policy attributes. Such attributes may include security and network parameters and network addresses. Gateway 380 has associated therewith a gateway administrator 310, who may manually modify various parameters within security configuration 370. However, such modifications may also be made automatically via software.

[0026] Client 320 does not have an associated administrator such as client administrator 101 in FIG. 1 above. According to embodiments of the present invention, client 320 need not maintain a security configuration corresponding to security configuration 370 of gateway 380.

[0027] Client 320 stores, has access to, or receives as input from a user, IP address 3[redacted] of gateway 380. Client 320 may maintain IP address 330 and a preshared secret or certificate for authentication. The preshared secret may be known to both client 320 and gateway 380 prior to negotiations which ultimately establish tunnel 350 within Internet 360.

[0028] FIG. 4 is a high-level flow diagram of method 400 according to an embodiment of the present invention. It is to be appreciated that method 400 may be implemented using various protocols. Moreover, additional negotiations (not shown) may be included in method 400.

[0029] In item 401, a client initiates a preliminary negotiation with a gateway. In item 410, the client initiates a second negotiation with the gateway. In some protocols, one negotiation may be initiated. The gateway sends information to the client in item 420. This information may have been requested by the client in a previous negotiation, such as in the negotiation initiated by the client in item 410. In item 430, the client extracts a security configuration from the information sent by the gateway. In item 435, the client initiates a final negotiation with the gateway. A tunnel providing secure communication between the client and the gateway is established in item 440 using the security configuration.

[0030] In item 420 of method 400, the gateway may also send information to the client about one or more protocols, such as the securID, RADIUS, and L2TP protocols. As such, the client may extract the information and use the protocols for additional negotiations. In an exemplary implementation (not shown), a security authentication negotiation may occur before item 435 in FIG. 4.

[0031] FIG. 5 is a high-level flow diagram of method 500 according to another embodiment of the present invention. In method 500, the IPSec protocol is employed to

establish a secure tunnel between a client and a gateway. In item 501, a phase1 negotiation occurs. The negotiation is described in further detail below. Phase1 negotiation may be effectuated using the Base Mode Exchange extension of the IPSec protocol, Internet Draft draft-ietf-ipsec-ike-base-mode-02.txt, as well as with Main Mode and Aggressive Mode, RFC 2409. As a result of phase1 negotiation, the client and the gateway authenticate each other and agree upon a valid security policy to govern a subsequent negotiation between the client and the gateway.

[0032] In item 510, an intermediate negotiation termed "phase1a" herein is initiated between the client and the gateway. In an exemplary implementation, phase1a negotiation utilizes the Configuration Mode Exchange extension, Internet Draft draft-dukes-ike-mode-cfg-00.txt, of the IPSec protocol. As a result of phase1a negotiation, the client receives from the gateway phase2 security parameters needed to negotiate phase2. In exemplary negotiations, the phase1 and phase2 parameters are independent of one another.

[0033] Because the client and the gateway now have identical security configurations, phase2 negotiation occurs in item 520. In some embodiments, Quick Mode, RFC 2409, an exchange of the IPSec protocol, may be employed. Assuming that phase2 negotiation succeeds, then the client and the gateway have generated secure keys to govern all subsequent transmissions between the client and the gateway. Therefore, in item 530, a tunnel has been established between the client and the gateway to enable secure communications.

[0034] FIG. 6 is a high-level flow diagram of method 600 according to an embodiment of the present invention. The dashed portions of method 600 may correspond to respective items within method 500 of FIG. 5.

[0035] Dashed portion A may correspond to phase1 negotiation in item 501. In accordance with the Base Mode Exchange extension of the IPSec protocol, a phase1 initiator may offer to a responder multiple security proposals containing multiple transforms, as well as the identity of the initiator, in the first packet of the negotiation.

[0036] In an exemplary implementation, a client may send to a gateway all or some permutations of the security algorithms supported by the client. Further, the proposals may be ordered within the transmitted packet from more to less secure proposals. As such, when the gateway parses these proposals, the more secure proposals may be considered before the less secure proposals. Accordingly, the highest level of security to govern subsequent negotiations may be selected. In addition, because the client offers all of its supported security attributes, phase1 negotiation will succeed—that is, a valid security policy will be matched—so long as the gateway supports at least one set of the proposed policies. Therefore, phase1 negotiation may occur successfully without the client storing, having access to, or receiving as input from a user, the security parameters the client must match for phase1 negotiation.

[0037] More specifically, in item 601 of FIG. 6, a client offers security proposals to a gateway when the client initiates a preliminary negotiation. In item 610, the gateway selects a proposal among the proposals offered by the client that matches a proposal supported by the gateway. The gateway may then send the selected proposal back to the client.

[0038] Dashed portion B of method 600 may correspond to phase1a negotiation in item 510 of FIG. 5. Configuration Mode Exchange of the IPSec protocol is based on a general request/reply protocol. An initiator makes a request of a responder, and the responder replies by sending back requested information to the initiator.

[0039] According to an embodiment of the present invention, the Configuration Mode Exchange extension is enhanced to include an additional set of attributes. In particular, the attributes include security attributes defining one or more phase2 security or policy associations. An initiator client needing configuration information requests that the responder gateway send all defined phase2 policies. Depending upon the configuration defined on the responder gateway, additional IPSec-related attributes and proprietary attributes may be sent by the gateway. The security attributes may also be sent along with traffic protected by each security association (SA). The phase2 security attributes may be designated with a prefix, such as "CFG_", so as to distinguish them from other information.

[0040] Once the client extracts the security configuration, including, for example, security and network parameters and identities, the client can use the configuration to initiate negotiations for all phase2 security associations defined on the gateway. Negotiations may succeed because attributes now known by the client match attributes defined on the gateway. In some embodiments, if the client already has phase2 policy definitions at the time the client initiates the negotiation, then the definitions are not used or are overwritten by software. In other embodiments, parameters evaluating to zero are not sent by the gateway in its reply to the client's request. Additionally, the number of iterations through each set of parameters may depend on the configuration of the client receiving the parameters. FIG. 7 illustrates an exemplary Configuration Mode Exchange transaction between a client and a gateway.

[0041] Specifically, in item 620 of FIG. 6, the client requests that the gateway send information, including all or some defined phase2 policies. In item 630, the gateway replies by sending the requested information back to the client. The information may be sent back in the form of sets of attributes, wherein each set contains sufficient information to define an IPSec security association. An attribute may be omitted from a given set, which may indicate

that no value exists for that attribute, that is, the attribute is not used. The number of sets of attributes returned by the gateway may be dictated by the configuration of the responder. In item 640, the client extracts security configuration information from the information sent by the gateway.

[0042] Dashed portion C may correspond to phase2 negotiation in item 520 of FIG. 5. In item 650, using the security configuration received by the client, the client and the gateway may negotiate phase2 security associations to generate secure keys. Differing levels of security may be applied to each SA. As such, multiple SAs may be used to enable a client to access multiple resources or services on a protected network. In item 660, a tunnel is established between the client and the gateway so that secure communications may occur between the client and the gateway.

[0043] The foregoing description of the preferred embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments are possible, and the generic principles presented herein may be applied to other embodiments as well. For instance, the IPSec protocol may continue to evolve, and various new or modified exchanges or extensions may be utilized to implement the present invention. Newly developed protocols may also be suitable. In other embodiments, a gateway may respond to a client by sending an IP address and security configuration of a second client or gateway. As such, a tunnel between the client and the second client or gateway may be established. In still other embodiments, a tunnel may be established between a first gateway and a second gateway.

[0044] Moreover, the invention may be implemented in part or in whole as a hard-wired circuit, as a circuit configuration fabricated into an application-specific integrated circuit, or

as a firmware program loaded into non-volatile storage or a software program loaded from or into a data storage medium as machine-readable code, such code being instructions executable by an array of logic elements such as a microprocessor or other digital signal processing unit.

[0045] As such, the present invention is not intended to be limited to the embodiments shown above but rather is to be accorded the widest scope consistent with the principles and novel features disclosed in any fashion herein.